



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/863,199	05/21/2001	Stephen P. Weeks	7451.0034-00	8932
22852	7590	11/15/2005		
FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP 901 NEW YORK AVENUE, NW WASHINGTON, DC 20001-4413			EXAMINER TRUONG, THANHNGA B	
			ART UNIT	PAPER NUMBER
			2135	
DATE MAILED: 11/15/2005				

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.		Applicant(s)	
	09/863,199		WEEKS ET AL	
	Examiner		Art Unit	
	Thanhnga B. Truong		2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 08/16/2005 (Amendment).
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-20 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-20 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 21 May 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date <u>7/29/05</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Applicant's amendment filed on August 16, 2005 has been entered. Claims 1-20 are pending. No claims are amended or canceled by the applicant.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 1-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Butt et al (US 6,754,829), and further in view of Griffin (US 5,958,050).

a. Referring to claim 1:

i. Butt teaches:

(1) obtaining a request for the computing resource; obtaining a group of certificates, each certificate expressing at least one authorization by at least one principal; identifying a set of principals associated with the certificates; initializing a state associated with each principal; evaluating a certificate as a function, at least in part, of the state associated with one or more of the principals; updating the state of one or more of the principals if the result of said evaluating step indicates that the state of a principal should be changed [**i.e., Figure 2 illustrates an authentication arrangement for one embodiment of the invention. Shown are a console computing device (console) 100, a core 102 computing device, a certificate authority (authority) 104, and a manageable device 106. Although only one manageable device 106 is illustrated, it is understood that many such will be present in a typical networked environment. The console is typically a computing device in use by an operator, where the operator seeks to manage the manageable device 106. The core 102 and certificate authority 104, as discussed below, allow the manageable device to validate the operator of the console, as well as any actions attempted by the operator. As illustrated, the core 102 and**

Art Unit: 2135

certificate authority 104 may be present within a single computing device, or they may be embodied in separate devices that are in communication with each other (column 5, lines 23-40). In addition, the core 102, by way of the certificate authority 104, issues operating system independent certificates to operators of consoles (e.g., console 100) which authenticate the identity of the console operators. As discussed above, the certificates embed a console operator's identity and group membership in the certificate, where access rights (in the form of access control lists) are stored at the manageable device(s) 106. The console operator proffers the certificate to a manageable device in support of a request to perform some management function. A manageable device 106, after receiving and validating the certificate, matches up the identity information within the certificate with the manageable device's local access control list information (column 5, lines 48-60)]; and

ii. Although Butt does not explicitly mention:

(1) repeating said evaluating and updating steps until a fixpoint is reached or until a predefined principal is found to authorize the request

iii. Griffin teaches:

(1) The trust manager will keep searching for a path through the web of claims, using hints as needed, moving up and down along a path as dead ends are encountered. Eventually, the trust manager may exhaust all possible hints and have searched all available claims. However, since nothing in the architecture of claims, certificates and hints demands that the web be finite and manageable, the trust manager is preferably programmed to limit the amount of time and computation expended in the search for a path. If such a limit is reached, the trust manager proceeds as if no path exists. Presumably, if a user finds that paths are only infrequently found, the user might reexamine the policy claims and loosen up on security if the user's system is too secure to be useful. Referring again to FIG. 3, the user can change the policy claims in TBF 132 or certificates in certificate repository 130 using class blesser 134 (column 9, lines 12-27).

iv. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) have applied the re-evaluating and re-updating steps in Butt to provide for management of trust relationships among code segments to be executed inside a trust boundary (**column 1, lines 23-25 of Griffin**).

v. The ordinary skilled person would have been motivated to:

(1) have applied the re-evaluating and re-updating steps in Butt because it is important to note that, when it comes to complex computer systems, trust is not just a matter of one's good faith or intentions. An otherwise trustworthy person may cause great damage to a computer system by making a mistake or running a program with bugs, viruses or Trojan horses. For this reason, robust computer systems are designed with the "principle of least authority" in mind. That principle dictates that a user or program should be granted only the authority needed to perform the task at hand and no more, to prevent intended and unintended ill effects (**column 1, lines 52-61 of Griffin**).

b. Referring to claim 2:

i. Butt further teaches:

(1) constructing a dependency graph, the dependency graph containing a node corresponding to each principal in the set of principals; and connecting at least two nodes in the dependency graph with a certificate that expresses a dependency of one node on the state of another node; wherein the dependency graph is used, at least in part, during said evaluating, updating, and repeating steps to determine which certificates to evaluate [**i.e., referring to Figure 7, this certificate is then marked 356 as a delegate certificate, and adds information in the additional information section of the certificate (see Figure 3) identifying the source of authority and delegation. The resulting session certificate can be used by the core to manage a manageable device 358 as session certificates would be used by a console operator. In addition, program modules include procedures, functions, programs, components, data structures, and the like, that perform particular tasks or implement particular abstract data types. The modules may be**

incorporated into single and multi-processor computing systems, as well as hand-held devices and controllable consumer devices. It is understood that modules may be implemented on a single computing device, or processed over a distributed network environment, where modules can be located in both local and remote memory storage devices (column 11, lines 43-67)].

c. Referring to claim 3:

i. This claim has limitations that is similar to those of claim 1, thus it is rejected with the same rationale applied against claim 1 above.

d. Referring to claim 4:

i. This claim has limitations that is similar to those of claims 1-2, thus it is rejected with the same rationale applied against claims 1-2 above.

e. Referring to claim 5:

i. Butt further teaches:

(1) in which the certificates comprise Simple Public Key Infrastructure certificates [i.e., referring to Figure 3, element 160].

f. Referring to claim 6:

i. Butt further teaches:

(1) in which the computing resource is one of: access to a piece of electronic content; use of a computer program; ability to execute a transaction; access to a computer; and access to a network [i.e., Figure 6 is a flowchart for a manageable device testing a request received from a console operator. At this point, a console operator has already contacted a core, proven identity (e.g., by the core checking the operator's login identity on the operator's console), and received a signed certificate allowing the operator to communicate with a particular manageable device. A manageable device receives 300 the request along with a session certificate (column 10, lines 15-65)].

g. Referring to claim 7:

i. This claim consists a computer program product for making trust management determinations to implement claim 1 and is rejected by the same prior art of record, wherein the limitation of a computer-readable medium for storing the

Art Unit: 2135

computer codes is disclosed in Figure 8, element 408, element 410, element 442, and element 444 (see also column 12, lines 13-18).

h. Referring to claim 8:

i. Butt further teaches:

(1) in which the computer readable medium is one of: CD-ROM, DVD, MINIDISC, floppy disk, magnetic tape, flash memory, ROM, RAM, system memory, network server, hard drive, optical storage, and a data signal embodied in a carrier wave [i.e., referring to Figure 8, element 408, element 410, element 442, and element 444 (see also column 11, lines 58-67)]. Furthermore, the storage systems and associated computer-readable media provide storage of data and executable instructions for the computing device 402. Note that storage options include hard-drives, floppy-disks, optical storage, magnetic cassettes, tapes, flash memory cards, memory sticks, digital video disks, and the like (column 12, lines 13-18)].

i. Referring to claim 9:

i. This claim consists a system for controlling access to electronic content or processing resources to implement claim 1 and is rejected by the same prior art of record.

j. Referring to claim 10:

i. Butt further teaches:

(1) a first computer system for processing requests for system resources, the first computer system comprising: a network interface for receiving digital certificates from other systems and for receiving requests to access electronic resources; a memory for storing electronic resources and one or more certificates relating thereto [i.e., referring to Figure 8, an exemplary system for implementing the invention includes a computing device 402 having system bus 404 for coupling together various components within the computing device. The system 404 bus may be any of several types of bus structures, such as PCI, AGP, VESA, Microchannel, ISA and EISA, etc. Typically, attached to the bus 402 are processors 406 such as Intel, DEC Alpha, PowerPC, programmable gate arrays,

etc., a memory 408 (e.g., RAM, ROM), storage devices 410, a video interface 416, input/output interface ports 418, and a network interface 420. It is understood that a modem 448 may operate in conjunction with an input port 418 to operate an alternative network interface. The storage systems and associated computer-readable media provide storage of data and executable instructions for the computing device 402. Note that storage options include hard-drives, floppy-disks, optical storage, magnetic cassettes, tapes, flash memory cards, memory sticks, digital video disks, and the like (column 12, lines 1-18)]; and

(2) a trust management engine for processing digital certificates and requests for electronic resources, and for making access control decisions by performing least fixpoint computations using said digital certificates [i.e., referring to Figure 6, The manageable device then verifies 302 that a trusted certificate authority associated with a core has signed the session certificate. Verification can be accomplished by using the issuer fields in the session certificate to lookup the certificate authority's certificate and verify that the session certificate was signed by the private key of the certificate authority (the core). Signature validation can be accomplished through application of known hash-check analysis on the signature, or by other techniques according to the nature of the signature. If 304 signature validation fails, then the manageable device ignores 306 all requests from the console. In one embodiment, the manageable device also sends an intruder detection warning to the core (column 10, lines 23-65)].

ii. Although Butt does not explicitly mention:

(1) performing at least fixpoint computations

iii. Griffin teaches:

(1) The trust manager will keep searching for a path through the web of claims, using hints as needed, moving up and down along a path as dead ends are encountered. Eventually, the trust manager may exhaust all possible hints and have searched all available claims. However, since nothing in the architecture of claims, certificates and hints demands that the web be finite and manageable, the

trust manager is preferably programmed to limit the amount of time and computation expended in the search for a path. If such a limit is reached, the trust manager proceeds as if no path exists. Presumably, if a user finds that paths are only infrequently found, the user might reexamine the policy claims and loosen up on security if the user's system is too secure to be useful. Referring again to FIG. 3, the user can change the policy claims in TBF 132 or certificates in certificate repository 130 using class blesser 134 (**column 9, lines 12-27**).

iv. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) have applied the fixpoint computations in Butt to provide for management of trust relationships among code segments to be executed inside a trust boundary (**column 1, lines 23-25 of Griffin**).

v. The ordinary skilled person would have been motivated to:

(1) have applied the fixpoint computations in Butt because it is important to note that, when it comes to complex computer systems, trust is not just a matter of one's good faith or intentions. An otherwise trustworthy person may cause great damage to a computer system by making a mistake or running a program with bugs, viruses or Trojan horses. For this reason, robust computer systems are designed with the "principle of least authority" in mind. That principle dictates that a user or program should be granted only the authority needed to perform the task at hand and no more, to prevent intended and unintended ill effects (**column 1, lines 52-61 of Griffin**).

k. Referring to claim 11:

i. Butt further teaches:

(1) a second computer system for making a request for system resources from the first computer system; a third computer system for generating a first digital certificate, the first digital certificate authorizing, at least in part, the second computer system to access a predefined system resource [**i.e., referring to Figure 8, it is understood that a remote computing device can be configured like computing device 402, and therefore may include many or all of the elements**

discussed for computing device 402. It should also be appreciated that remote computing devices 442 may be embodied separately, or combined within a single device; for example, a core and certificate authority may be combined into a single device which coordinates a console operator's access to a particular manageable device (column 12, lines 36-45)].

l. Referring to claims 12, 13:

i. These claims consist additional system for controlling access to electronic content or processing resources to implement claim 11 and is rejected by the same prior art of record.

m. Referring to claim 14:

i. Butt further teaches:

(1) in which the first computer system further comprises a public key associated with the fourth computer system, the public key corresponding to a private key used to sign the second digital certificate [i.e. referring to Figure 3, element 160 and element 352 of Figure 7. In addition, the manageable device can also verify that the console operator has the private key associated with the public key embedded within the received session certificate (column 10, lines 36-39)].

n. Referring to claims 15-16:

i. These claims have limitations that is similar to those of claim 5, thus they are rejected with the same rationale applied against claim 5 above.

o. Referring to claim 17:

i. This claim consists a method for performing trust management computation to implement claims 1 and 9, and is rejected by the same prior art of record.

p. Referring to claim 18:

i. Butt further teaches:

(1) in which the structure comprises a lattice [i.e., Figure 3 represents a lattice structure. Traditional certificate content includes the Subject Name 156, public key 160, certificate serial number 162 (this can be used

Art Unit: 2135

by the certifying authority to look up the certificate), certificate validity date 164, certificate authority (e.g., issuer) identifier 166, and a digital signature 168 for the certifying authority. The digital signature is a private key (in a public key cryptosystem) encryption of the digest computed on the contents of the certificate. This signature can be validated by anyone holding the associated public key for the private key. The extended data 154 includes a username and group membership for that name. This information is placed in the certificate by the certificate authority 104, and is based on the namespace of the core 102 (column 7, lines 64-67 through column 8, lines 1-12)].

q. Referring to claim 19:

i. Butt further teaches:

(1) in which the structure is chosen such that it provides an ordering for authorizations, a way to combine authorizations, and a way to express certificates as monotone functions [i.e., when the manageable device is presented a certificate, and after it validates the certificate, it compares the username and group membership information to an access control list to determine whether to allow operations requested by the operator (column 8, lines 12-16)].

r. Referring to claim 20:

i. This claim has limitations that is similar to those of claims 18-19, thus it is rejected with the same rationale applied against claims 18-19 above.

Response to Argument

4. Applicant's arguments filed August 16, 2005 have been fully considered but they are not persuasive.

Applicant argues that:

"The cited art fails to show or suggest the claimed invention, either individually or in combination, as each of the '829 and '050 patents fail to show or suggest the elements of the pending claims without impermissible hindsight. As noted in detail above, the '829 patent fails to show or suggest many of the elements recited in the pending claims, especially the unique elements of using fixpoint computations and updating the states of the principals."

Examiner respectfully disagrees with the applicant and still maintains that:

The combination of teaching between Butt and Griffin teach the claimed subject matter. Butt's invention discloses in one embodiment, methods and apparatus for an operator of a console to authenticate to a system of heterogeneous computers by logging in only once to a representative computer or "core". After logging in, the operator acquires a session certificate (e.g., an X.509-based certificate), allowing the operator to prove identity and group membership information to other nodes on a network. The core, before signing session certificates, embeds data in an extended data area of the certificates. The extended data includes the operator's username and groups to which the operator belongs, and possibly other information such operator context (or domain). The username, group membership, and other extended data is based on the namespace of the core computer, and other devices on the network need not belong to that namespace or even use the same network operating system. Manageable devices can authenticate and authorize access to themselves based on the extended data submitted to them by the bearer of a session certificate. Authenticity and ownership of the certificate is verified using standard public key cryptosystem methods. In some embodiments, manageable devices verify operator authorization by cross-referencing operator identity and group membership information in the certificate with an appropriate access control list (or equivalent data structure). In some embodiments, manageable devices are pre-configured to trust at least one core by giving it the public key of the core, and the core can direct the manageable device to trust other cores (see Butt's abstract). On the other hand, Griffin teaches a trust manager examines each new class before it is allowed to execute by examining a policy file which includes data structures defining security policies of the user system, a certificate repository for storing a plurality of certificates, a certificate being a data record which is digitally signed and which certifies claims relevant to a security evaluation, a code examiner adapted to analyze the portion of code to determine potential resource use of the portion of code and a trust evaluator adapted to evaluate certificate requirements of the portion of code based on policy rules extracted from the policy file and the potential resource use specified by the code examiner. The trust evaluator also

Art Unit: 2135

determines, from certificates from the certificate repository and a code identifier identifying the portion of code, whether execution of the portion of code is allowed by the policy rules given the potential resource use, the code supplier and applicable certificates. Certificates and policies can be specified in hierarchical form, so that some levels of security can be delegated to trusted entities (see Griffin's abstract). Specially, Griffin states that the trust manager will keep searching for a path through the web of claims, using hints as needed, moving up and down along a path as dead ends are encountered. Eventually, the trust manager may exhaust all possible hints and have searched all available claims. However, since nothing in the architecture of claims, certificates and hints demands that the web be finite and manageable, *the trust manager is preferably programmed to limit the amount of time and computation expended in the search for a path. If such a limit is reached, the trust manager proceeds as if no path exists (emphasis added)*. Presumably, if a user finds that paths are only infrequently found, the user might reexamine the policy claims and loosen up on security if the user's system is too secure to be useful. Referring again to FIG. 3, the user can change the policy claims in TBF 132 or certificates in certificate repository 130 using class blesser 134 **(column 9, lines 12-27)**. Clearly the combination teaching between Butt and Griffin is proper.

In response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971). Besides, Butt and Griff do not need to disclose anything over and above the invention as claimed in order to render it unpatentable or anticipate. A recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. If the

prior art structure is capable of performing the intended use, then it meets the claimed limitations.

For the above reasons, it is believed that the rejections should be sustained.

Conclusion

5. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 571-272-3858.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The central fax number for the organization where this application or proceeding is assigned is 571-273-8300.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

TBT

November 2, 2005


KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100